HYBRIDIZATION OF STEGANOGRAPHY AND CRYPTOGRAPHY

AVISHEK MITRA

ROLL-NO:115/CSC/211030

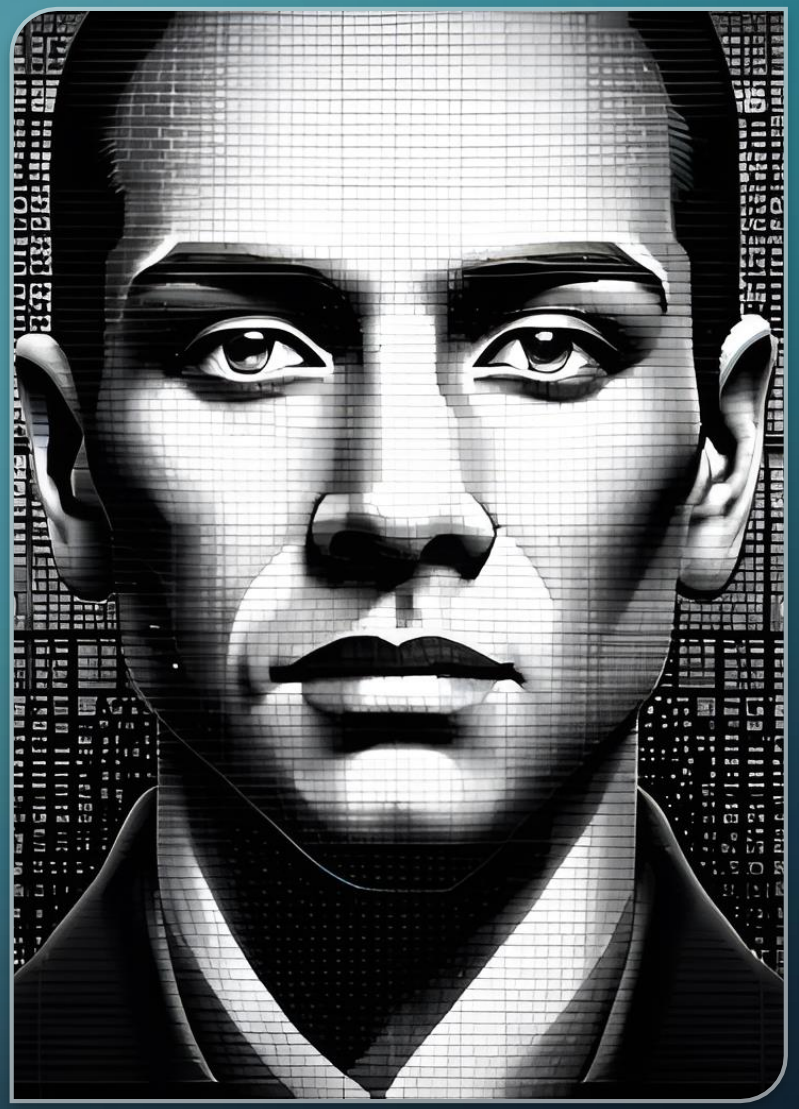
ADITI BHATTACHARJEE
Roll No: 115/CSC/211027

DOMAIN DESCRIPTION

With the rapid growth of digitization, providing security to information over Internet is most challenging. Three major security goals include Confidentiality, Integrity and Availability. Confidentiality is probably the most important among three.

Steganography and Cryptography plays a vital role in providing security to the information in transit.

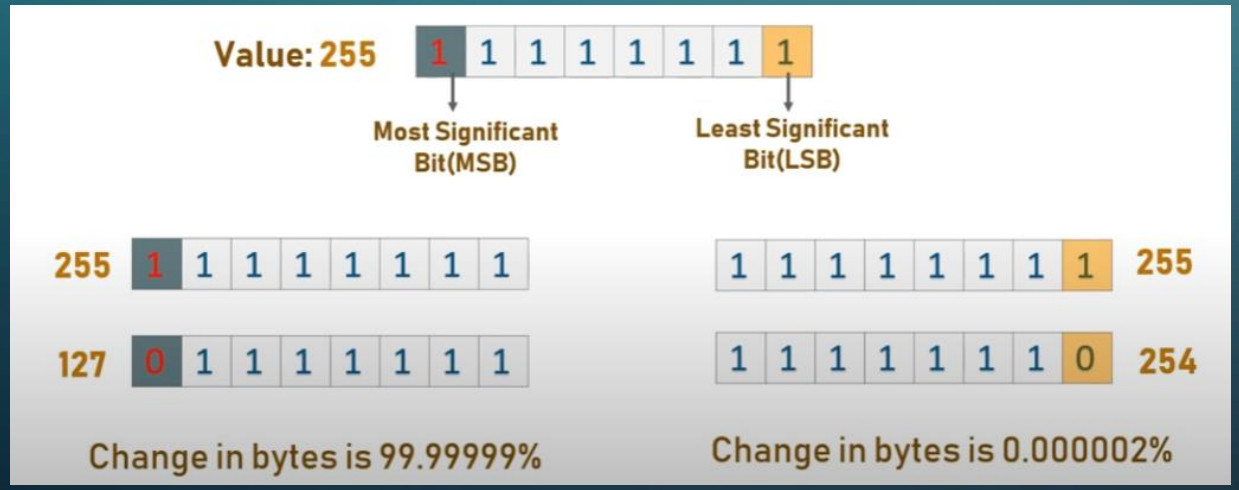
So we want to combine Steganography and Cryptography approach and build a new algorithm of this two approach to provide a better security .

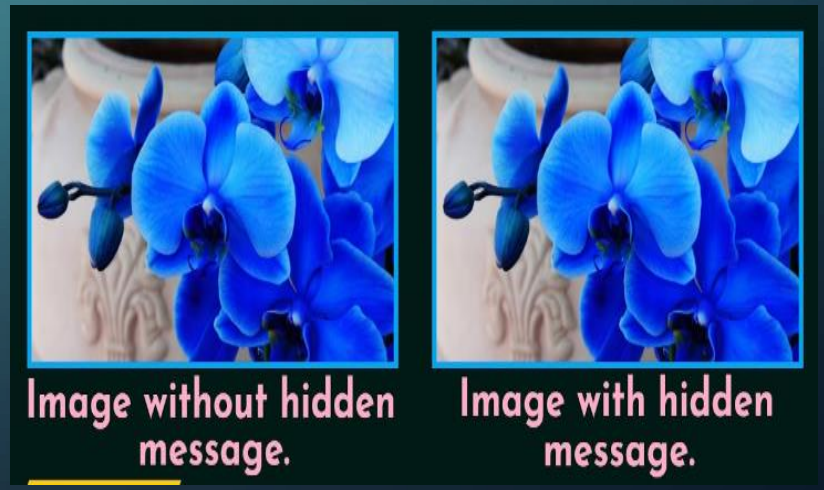


INTRODUCTION

WHAT IS STEGANOGRAPHY ?

Steganography is a technique used to hide secret information within other ordinary-looking data, such as images, audio files, or text, in a way that is not easily detectable. It's like hiding a message inside another message so that only the intended recipient knows it exists. The goal is to make the hidden information blend in seamlessly with its surroundings, making it difficult for anyone else to notice or decipher. Steganography is often used to protect sensitive data or to send covert messages securely without drawing attention.





WHAT IS CRYPTOGRAPHY

- Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it.In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it.

Features Of Cryptography

- **Confidentiality**
- **Integrity**
- **Authentication**

Types Of Cryptography:

. Symmetric Key Cryptography
. Hash Functions
. Asymmetric Key Cryptography

WHY COMBINE STEGANOGRAPHY WITH ENCRYPTION?

- Combining steganography with encryption can provide an extra layer of security when transmitting sensitive information. By hiding the message within another message and then encrypting it, even if someone intercepts the transmission, they will not be able to read the message without the decryption key.
- In addition, combining these two techniques can also make it more difficult for attackers to detect that a hidden message even exists, as the message is concealed within another innocuous message.

MOTIVATION AND SCOPE OF THE WORK

- Now this time security is a crucial thing in our day-to-day life. The common encryption and steganographic approach should be cracked. That's why we build a new steganography and cryptography approach to provide better security. We combine these two new approaches and make dual security.

1. **Increased Confidentiality**
2. **Covert Communication**
3. **Dual-Layered Security**
4. **Defense against Attacks**

SCOPE OF THE WORK:

- **Algorithm Development :** Designing and developing steganographic & encryption algorithms that can effectively embed encrypted data into carrier media.
- **Performance Optimization :** Optimizing the performance of the combined system to ensure efficient embedding and extraction processes, minimizing any potential impact on the carrier media or overall system performance.
- **Security Analysis:** Evaluating the robustness and security of the combined steganography and encryption system against various attacks, such as statistical analysis, brute-force attacks, or detection algorithms.

BACKGROUND/REVIEW OF RELATED WORK

- In the last few years, the researchers have shown the impact of Steganography and Cryptography on the real life events and needs in their research activities. Moreover, a notable amount of works have been proposed in the related fields to monitor the effect of the same.

[1] Forouzan, B. A., & Mukhopadhyay, D. (2011). Cryptography and network security :We have learned about cryptography and its variations. We are gathering knowledge about encryption and decryption algorithms.

[2] Hamid, Nagham, Abid Yahya, R. Badlishah Ahmad, and Osamah M. Al- Qershi. "Image steganography techniques: Here we learn about steganography technique, working with whole value of all pixels .

[3] Mishra, Rina, and Praveen Bhanodiya. "A review on steganography and cryptography: In this paper they have used DES as an encryption algorithm and common LSB algorithm for steganography.

Etc…

After studying about these papers and works we gather our knowledge and help us build our algorithm.

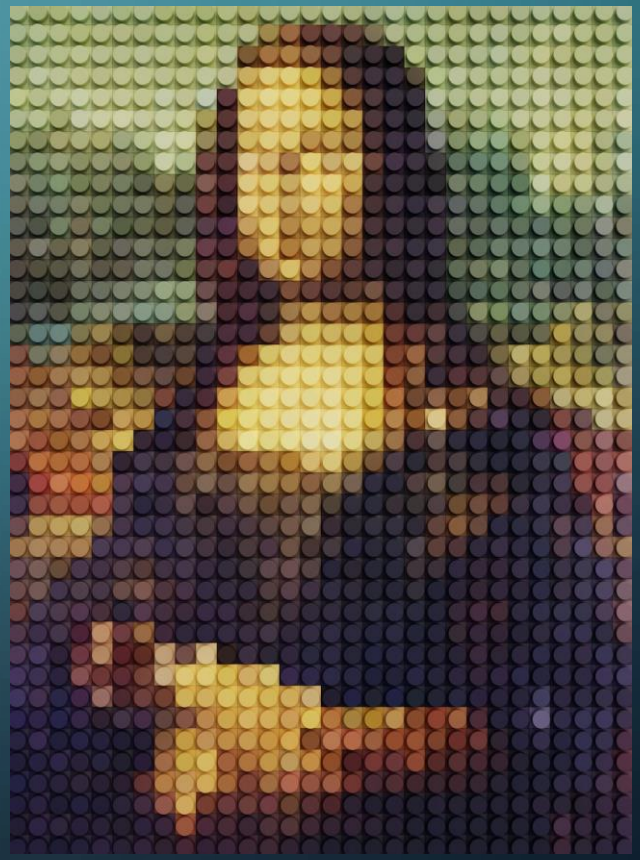
METHODOLOGY

PROBLEM FORMULATION :

Nowadays weak encryption or the absence of encryption can make data more vulnerable to unauthorized access or interception. Without robust encryption or steganography, personal privacy can be compromised. Communication, including emails, messages, or file transfers, can be intercepted and monitored, violating individuals' privacy rights and confidentiality.

Algorithm Description

Pixel difference Steganographic algorithm: Pixel difference steganography is a technique that hides information within the differences between adjacent pixels in a digital image. Instead of modifying the pixel values directly, this approach focuses on manipulating the variations between neighboring pixels.



PROPOSED STEGANOGRAPHIC ENCODING ALGORITHM:

Assume the matrix is this and the message is 1011.

2	7	10	15
4	8	11	2
6	7	9	5
13	3	1	8

- First 2 pixel value is 2 & 7
- The difference between them |2-7|=5=00000101

- The first bit of the msg is 1.
- The lsb of the difference is 1.
- So ,nothing will change.

2	7	9	15
4	8	11	2
6	7	9	5
13	3	1	8

- Next 2 pixel value is 7 & 10
- The difference between them |7-10|=3=00000011

- The next bit of the msg is 0.
- The lsb of the difference is 1.
- So , we change the lsb by 0
- now difference is 00000010=2
- So , we change the difference and make it 2
- That's why we decrement next pixel by 1 and make it 9.

PROPOSED VOWEL TEXT ENCRYPTION ALGORITHM

PLAIN TEXT: HELLO WORLD

Adding starting, ending, separator and padding character

αHELLOϕWORLDβγγγ

Plaintext to be encrypted using Key: **αHELLOϕW**

Key 1 : 10203040506070809011121314

Cipher Text Generated: 10112090206030903090406020111012

	10	20	30	40	50
60	A	E	I	O	U
70	B	F	J	P	V
80	C	G	K	Q	W
90	D	H	L	R	X
11	α	β	M	S	Y
12	γ	ϕ	N	T	Z
13	0	1	2	3	4
14	5	6	7	8	9

Key Generation:

Initial Key	10	20	30	40	50	60	70	80	90	11	12	13	14
Bit Representation	0000 1010	0001 0100	0001 1110	0010 1000	0011 0010	0011 1100	0100 0110	0101 0000	0101 1010	0000 1011	0000 1100	0000 1101	0000 1110
1 bit cycle	0000 0101	0000 1010	0000 1111	0001 0100	0001 1001	0001 1110	0010 0011	0010 1000	0010 1101	0000 0101	0000 0110	0000 0110	0000 0111
Integer representation	05	10	15	20	25	30	35	40	45	05	06	06	07

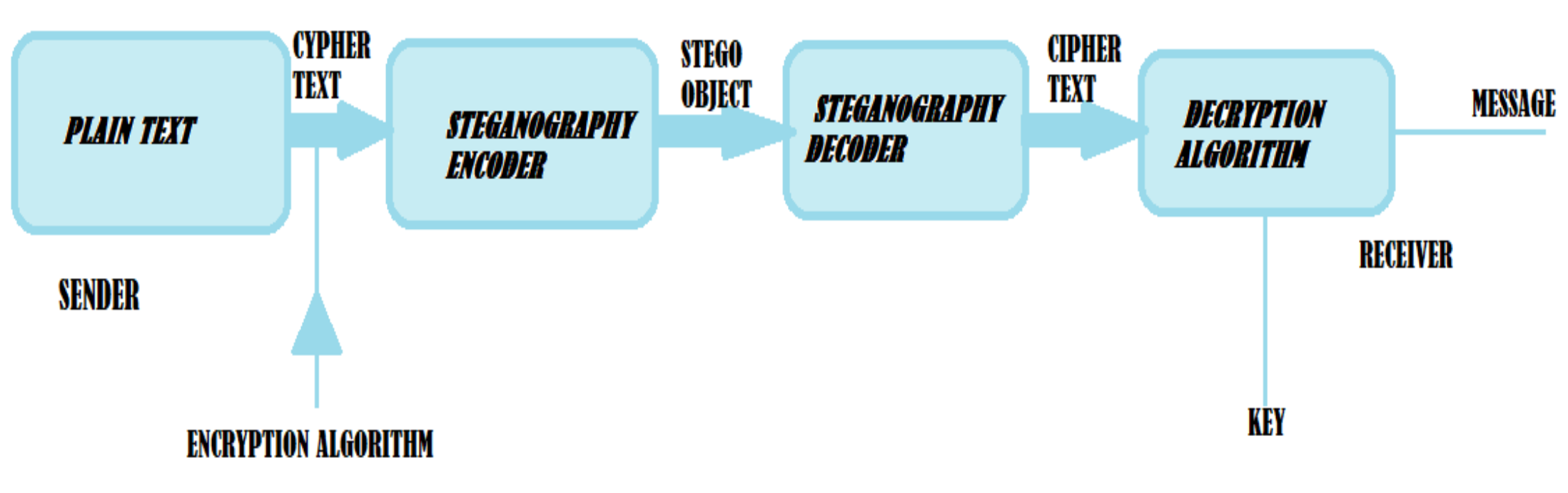
Plaintext to be encrypted using Key: **ORLDβγγγ**

Key 2 :05101520253035404505060607

	05	10	15	20	25
30	A	E	I	O	U
35	B	F	J	P	V
40	C	G	K	Q	W
45	D	H	L	R	X
05	α	β	M	S	Y
06	γ	ϕ	N	T	Z
06	0	1	2	3	4
07	5	6	7	8	9

Cipher Text Generated:203020451545054510050506050605 06

IMPLEMENTATION



RESULT AND DISCUSSION

- **Sender side:**
- **Encrypt the data:**
- Write the message which we want to send.
- Write the private key for encryption.

```
Enter 1 to encrypt and 2 to decrypt: 1
Enter plain text: AVISHEK ADITI
enter key:10203040506070809011121314
the key: 10203040506070809011121314
Encrypted Text: 10111060507030604011209020603080643632923233969228369692323632 36
```

- Finally, the plain text is transformed into the cipher text.

. Embed the Encrypted Data:

. Choose the image where we want to hide the cipher text.
. Then put the cipher text to hide it.
. Select a name for the steganographic image and store it.

```
Enter choice 1- Encode, 2-Decode1
Enter image path: lena.png
Enter Text to hide: 10111060507030604011209020603080643632923233969228369692323632 36
Enter image path to save image: 1.png
```

RESULT

PICTURE 4 is the image that is selected as a medium and PICTURE 5 is the image that is generated after the steganographic technique.

PICTURE A

PICTURE B

Receiver side:

Steganographic decoding:

. Choose the image which the receiver gets and using Steganographic decoding get the cipher text.

```
Enter choice 1- Encode, 2-Decode2
Enter image path: 1.png
10111060507030604011209020603080643632923233969228369692323632 36
```

Decryption:

. Enter the cipher text which we get in the previous step.

. Enter the private key to decrypt the cipher text.

Finally, we got the actual message which is sent by the sender.

```
Enter 1 to encrypt and 2 to decrypt: 2
Enter Cipher text: 10111060507030604011209020603080643632923233969228369692323632 36
Enter Key: 102030405060708090111213 14
AVISHEK ADITI
```

DISCUSSION

- After getting the result by using our proposed steganography and encryption algorithm
- we can say that our technique maintains confidentiality in better form.
- encoding the data only in LSB is now a little bit easy to retrieve it. So our new approach can make it more difficult and provide more security to hide our data in the image. For this, the out image has a very minor difference from the input image.
- In our proposed algorithm, Key Size is calculated by multiplying the number of rows and the number of columns by 8. Here, the number of rows is 5 and the number of columns is 8; summing to 13. Each index is represented using 8 bits. So, the total number of bits used to represent the key becomes 104 bits (13 X 8 bits).
- The combination of steganography and encryption provides an additional layer of security to protect sensitive information. The implemented solution ensures that the encrypted data is concealed within a carrier medium, making it difficult for unauthorized individuals to detect or access the hidden information.

REFERENCES

. [1] Provos, Niels, and Peter Honeyman. "Hide and seek: An introduction to steganography." *IEEE security & privacy* 1, no. 3 (2003): 32-44.

- [2] Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. "An overview of image steganography." In *ISSA*, vol. 1, no. 2, pp. 1-11. 2005.
- [3] Forouzan, B. A., & Mukhopadhyay, D. (2011). Cryptography and network security (Sie). McGraw-Hill Education.
- [4] Laskar, Shamim Ahmed, and Kattamanchi Hemachandran. "High Capacity data hiding using LSB Steganography and Encryption." *International Journal of Database Management Systems* 4, no. 6 (2012): 57.
- [5] Hamid, Nagham, Abid Yahya, R. Badlishah Ahmad, and Osamah M. Al- Qershi. "Image steganography techniques: an overview." *International Journal of Computer Science and Security (IJCSS)* 6, no. 3 (2012): 168-187.
- [6] Bloisi, Domenico Daniele, and Luca Iocchi. "Image based steganography and cryptography." In *VISAPP (1)*, pp. 127-134. 2007.
- [7] Mishra, Rina, and Praveen Bhanodiya. "A review on steganography and cryptography." In *2015 International Conference on Advances in Computer Engineering and Applications*, pp. 119-122. IEEE, 2015.

THANK YOU.